ABSTRACT OF THE DISCLOSURE

When sending personal data to a recipient, the data owner encrypts the data using both a public data item provided by a trusted party and an encryption key string formed using at least policy data indicative of conditions to be satisfied before access is given to the personal data. The encryption key string is typically also provided to the recipient along with the encrypted personal data. To decrypt the personal data, the recipient sends the encryption key string to the trusted party with a request for the decryption key. The trusted party determines the required decryption key using the encryption key string and private data used in deriving its public data, and provides it to the requesting recipient. However, the decryption key is either not determined or not made available until the trusted party is satisfied that the associated policy conditions have been met by the recipient.